CEIC® 2014

Overview

What is Defrag?

How does it relate to spoliation?

How can Defrag be run?

Manual Execution Artifacts

Automatic Execution Artifacts

CEIC 2014

Defrag

A built in Windows tool for defragmenting files

Speeds up Read/Write operations

Can run automatically depending on the OS version

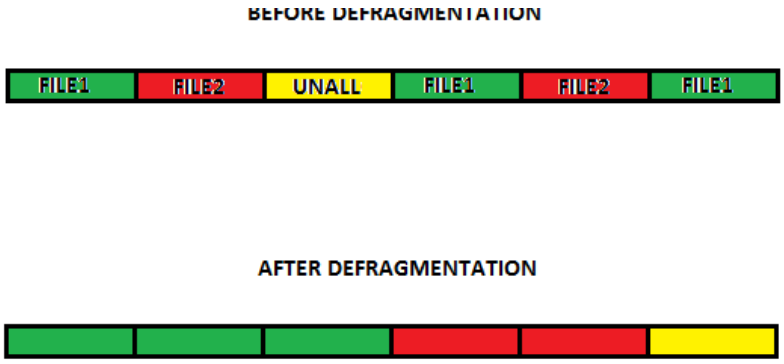
CEIC 2014

Spoliation

Black's Law Dictionary: The **spoliation of evidence** is the intentional or negligent withholding, hiding, altering, or destroying of evidence relevant to a legal proceeding.

CEIC 2014

Defrag Overview



CEIC 2014

How is it invoked?

Different ways to start a defrag process (Auto as a system process, Scheduled task, Manually from GUI, Manually from Command Line)

When it is invoked by different methods, different evidence is present.

CEIC 2014

The search for execution…

What areas can we examine for artifacts of program execution?

Prefetch files

Userassist Key in the registry

Other Reg files

Event Logs

CEIC 2014

Prefetch Files

Prefetch in brief

What files are we looking for?

DFRGNTFS.EXE - XP/VISTA

DEFRAG.EXE - XP/VISTA/7

DRFGUI.EXE - VISTA/7

MMC.EXE - XP

CMD.EXE – XP/7/VISTA

CEIC 2014

XP Prefetch Files

If the process is run manually through the GUI, we would expect to see DFRGNTFS.EXE and MMC.EXE but NOT DEFRAG.EXE

If the process is run manually from the command line, we would expect to see DFRGNTFS.EXE, CMD.EXE and DEFRAG.EXE

If the process is run automatically, we would expect to see DFRGNTFS.EXE and DEFRAG.EXE

CEIC 2014

XP Manually through the GUI

Prefetch File Name	Executable	Run Count	UTC Time
AXLBRIDGE.EXE-3854FF27.pf	AXLBRIDGE.EXE	4	Tue Oct 8 18:05:53 2013
DFRGNTFS.EXE-38C3807C.pf	DFRGNTFS.EXE	1	Sun Oct 6 01:08:53 2013
DLG.EXE-332F77D1.pf	DLG.EXE	1	Wed Oct 9 14:53:01 2013
DLLHOST.EXE-1D37383A.pf	DLLHOST.EXE	1	Sat Oct 5 15:08:29 2013
DOCPROC.EXE-039645B2.pf	DOCPROC.EXE	11	Mon Oct 7 20:18:30 2013
DPE_OCR.EXE-0C157E74.pf	DPE_OCR.EXE	4	Mon Oct 7 20:18:42 2013
EXCEL.EXE-1FF53647.pf	EXCEL.EXE	1	Mon Oct 7 18:30:03 2013
MMC.EXE-53159585.pf	MMC.EXE	1	Sun Oct 6 01:08:52 2013

CEIC 2014

XP From Command Line

Prefetch File Name	Executable	Run Count	UTC Time
AXLBRIDGE.EXE-3854FF27.pf	AXLBRIDGE.EXE	4	Tue Oct 8 18:05:53 2013
CMD.EXE-034B0549.pf	CMD.EXE	4	Sun Oct 6 01:08:42 2013
DEFRAG.EXE-2858C7E2.pf	DEFRAG.EXE	1	Sun Oct 6 01:08:53 2013
DFRGNTFS.EXE-38C3807C.pf	DFRGNTFS.EXE	1	Sun Oct 6 01:08:53 2013
DLG.EXE-332F77D1.pf	DLG.EXE	1	Wed Oct 9 14:53:01 2013
DLLHOST.EXE-1D37383A.pf	DLLHOST.EXE	1	Sat Oct 5 15:08:29 2013
DOCPROC.EXE-039645B2.pf	DOCPROC.EXE	11	Mon Oct 7 20:18:30 2013
DPE_OCR.EXE-0C157E74.pf	DPE_OCR.EXE	4	Mon Oct 7 20:18:42 2013
EXCEL.EXE-1FF53647.pf	EXCEL.EXE	1	Mon Oct 7 18:30:03 2013

CEIC 2014

XP System Invoked

Prefetch File Name	Executable	Run Count	UTC Time
AXLBRIDGE.EXE-3854FF27.pf	AXLBRIDGE.EXE	4	Tue Oct 8 18:05:53 2013
DEFRAG.EXE-2858C7E2.pf	DEFRAG.EXE	1	Sun Oct 6 01:08:53 2013
DFRGNTFS.EXE-38C3807C.pf	DFRGNTFS.EXE	1	Sun Oct 6 01:08:53 2013
DLG.EXE-332F77D1.pf	DLG.EXE	1	Wed Oct 9 14:53:01 2013
DLLHOST.EXE-1D37383A.pf	DLLHOST.EXE	1	Sat Oct 5 15:08:29 2013
DOCPROC.EXE-039645B2.pf	DOCPROC.EXE	11	Mon Oct 7 20:18:30 2013
DPE_OCR.EXE-0C157E74.pf	DPE_OCR.EXE	4	Mon Oct 7 20:18:42 2013
EXCEL.EXE-1FF53647.pf	EXCEL.EXE	1	Mon Oct 7 18:30:03 2013

CEIC 2014

Vista Prefetch Files

If the process is run manually through the GUI we would expect to see DEFRAG.EXE, DFRGNTFS.EXE and DFRGUI.EXE

If the process is run manually from the command line, we would expect to see DFRGNTFS.EXE, CMD.EXE and DEFRAG.EXE

If the process is run automatically we would expect to see DEFRAG.EXE and DFRGNTFS.EXE

CEIC 2014

Vista Manually through the GUI

Prefetch File Name	Executable	Run Count	UTC Time
AXLBRIDGE.EXE-3854FF27.pf	AXLBRIDGE.EXE	4	Tue Oct 8 18:05:53 2013
CMD.EXE-034B0549.pf	CMD.EXE	4	Fri Oct 4 14:51:29 2013
DEFRAG.EXE-2858C7E2.pf	DEFRAG.EXE	1	Sun Oct 6 01:08:53 2013
DFRGNTFS.EXE-38C3807C.pf	DFRGNTFS.EXE	1	Sun Oct 6 01:08:53 2013
DFRGUI-1F3E9D7E.pf	DFRGUI.EXE	1	Sun Oct 6 01:08:53 2013
DLLHOST.EXE-1D37383A.pf	DLLHOST.EXE	1	Sat Oct 5 15:08:29 2013
DOCPROC.EXE-039645B2.pf	DOCPROC.EXE	11	Mon Oct 7 20:18:30 2013
DPE_OCR.EXE-0C157E74.pf	DPE_OCR.EXE	4	Mon Oct 7 20:18:42 2013
EXCEL.EXE-1FF53647.pf	EXCEL.EXE	1	Mon Oct 7 18:30:03 2013

CEIC 2014

Win7 Prefetch Files

If the process is run manually through the GUI we would expect to see DFRGUI.EXE

If the process is run manually from the command line we would expect to see DEFRAG.EXE and CMD.EXE

If the process is run automatically we would expect to see DEFRAG.EXE

CEIC 2014

Win7 Manually through the GUI

Prefetch File Name	Executable	Run Count	UTC Time
AXLBRIDGE.EXE-3854FF27.pf	AXLBRIDGE.EXE	4	Tue Oct 8 18:05:53 2013
CMD.EXE-034B0549.pf	CMD.EXE	4	Fri Oct 4 14:51:29 2013
DFRGUI-1F3E9D7E.pf	DFRGUI.EXE	1	Sun Oct 6 01:08:53 2013
DLLHOST.EXE-1D37383A.pf	DLLHOST.EXE	1	Sat Oct 5 15:08:29 2013
DOCPROC.EXE-039645B2.pf	DOCPROC.EXE	11	Mon Oct 7 20:18:30 2013
DPE_OCR.EXE-0C157E74.pf	DPE_OCR.EXE	4	Mon Oct 7 20:18:42 2013
EXCEL.EXE-1FF53647.pf	EXCEL.EXE	1	Mon Oct 7 18:30:03 2013

CEIC 2014

Win7 From Command Line

Prefetch File Name	Executable	Run Count	UTC Time
AXLBRIDGE.EXE-3854FF27.pf	AXLBRIDGE.EXE	4	Tue Oct 8 18:05:53 2013
CMD.EXE-034B0549.pf	CMD.EXE	1	Sun Oct 6 01:08:45 2013
DEFRAG.EXE-2858C7E2.pf	DEFRAG.EXE	1	Sun Oct 6 01:08:53 2013
DLLHOST.EXE-1D37383A.pf	DLLHOST.EXE	1	Sat Oct 5 15:08:29 2013
DOCPROC.EXE-039645B2.pf	DOCPROC.EXE	11	Mon Oct 7 20:18:30 2013
DPE_OCR.EXE-0C157E74.pf	DPE_OCR.EXE	4	Mon Oct 7 20:18:42 2013
EXCEL.EXE-1FF53647.pf	EXCEL.EXE	1	Mon Oct 7 18:30:03 2013

CEIC 2014

Win7 System Invoked

Prefetch File Name	Executable	Run Count	UTC Time
AXLBRIDGE.EXE-3854FF27.pf	AXLBRIDGE.EXE	4	Tue Oct 8 18:05:53 2013
CMD.EXE-034B0549.pf	CMD.EXE	4	Fri Oct 4 14:51:29 2013
DEFRAG.EXE-2858C7E2.pf	DEFRAG.EXE	1	Sun Oct 6 01:08:53 2013
DLLHOST.EXE-1D37383A.pf	DLLHOST.EXE	1	Sat Oct 5 15:08:29 2013
DOCPROC.EXE-039645B2.pf	DOCPROC.EXE	11	Mon Oct 7 20:18:30 2013
DPE_OCR.EXE-0C157E74.pf	DPE_OCR.EXE	4	Mon Oct 7 20:18:42 2013
EXCEL.EXE-1FF53647.pf	EXCEL.EXE	1	Mon Oct 7 18:30:03 2013

CEIC 2014

UserAssist

UserAssist in brief

What execution are we looking for?

Disk Defragmenter.lnk – XP

Dfrgui.lnk – VISTA/WIN7

CEIC 2014

Other Registry Keys

SOFTWARE\Microsoft\Dfrg\BootOptimizeFunction

NTUSER\Software\Microsoft\Microsoft Management Console\Recent File List

CEIC 2014

BootOptimizeFunction

CEIC 2014

Event Logs

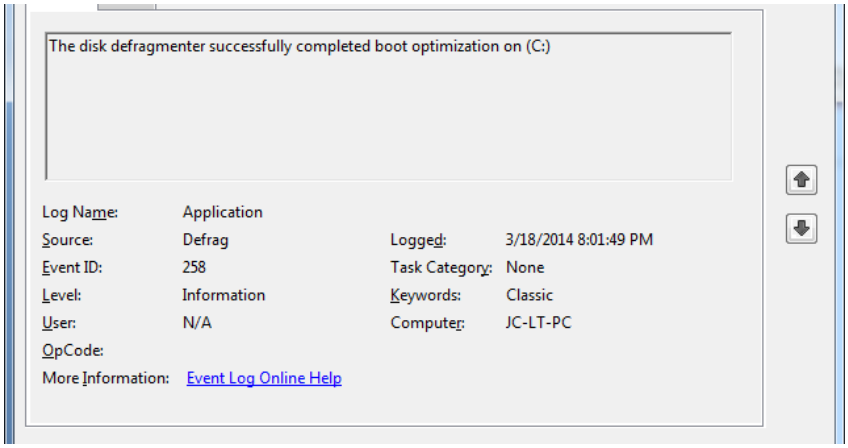
No logging for defrag events in Windows XP

Logging for defrag is present in Windows Vista and Windows 7

Logging of Scheduled Tasks as well as Defrag Service

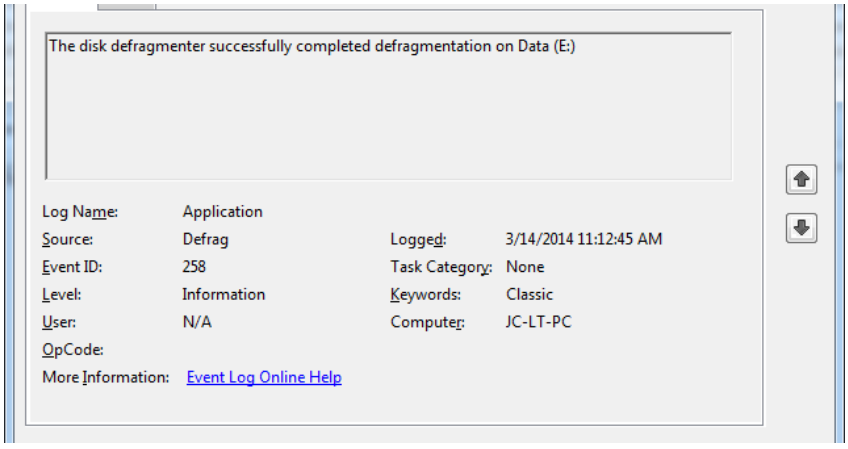
CEIC 2014

Windows 7 Event Log BootOptimize



CEIC 2014

Windows 7 Event Log Normal



CEIC 2014

Solid State

Solid State drives don't need defrag

Don't contain all the artifacts we talked about

May still see evidence of defrag in Event Logs

CEIC 2014

Thanks for Listening!

John Cotton

Computer Evidence Recovery

John@computerpi.com